SIMMONS HANLY CONROY, LLC
Jason 'Jay' Barnes (admitted *pro hac vice*)
An Truong (admitted *pro hac vice*)
Eric Johnson (admitted *pro hac vice*)
112 Madison Avenue, 7th Floor
New York, NY 10016
Telephone: (212) 784-6400
Facsimile: (212) 213-5949
jaybarnes@simmonsfirm.com
atruong@simmonsfirm.com
ejohnson@simmonsfirm.com

KIESEL LAW LLP
Jeffrey A. Koncius, State Bar No. 189803
Nicole Ramirez Jones, State Bar No. 279017
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
koncius@kiesel.law
ramirezjones@kiesel.law

SCOTT+SCOTT ATTORNEYS AT LAW LLP
Joseph P. Guglielmo (admitted *pro hac vice*)
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 233-4565
Facsimile: (619) 233-0508
jguglielmo@scott-scott.com

LOWEY DANNENBERG, P.C.
Christian Levis (admitted *pro hac vice*)
Amanda Fiorilla (admitted *pro hac vice*)
44 South Broadway, Suite 1100
White Plains, NY 10601
Telephone: (914) 997-0500
Facsimile: (914) 997-0035
clevis@lowey.com
afiorilla@lowey.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Michael W. Sobol, State Bar. No. 194857
Melissa Gardner, State Bar No. 289096
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008
msobol@lchb.com
mgardner@lchb.com

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP
Douglas Cuthbertson (admitted *pro hac vice*)
250 Hudson Street, 8th Floor
New York, NY 10013
Telephone: (212) 355-950
Facsimile: (212) 355-9592
dcuthbertson@lchb.com

Attorneys for Plaintiffs and the Proposed Class
Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

JOHN DOE, *et al.*, individually and on behalf of all others similarly situated, Plaintiffs, GOOGLE LLC, Defendant.	Case No. 3:23-cv-02431-VC **PLAINTIFFS' RESPONSE IN OPPOSITION TO GOOGLE'S MOTION TO DISMISS SECOND AMENDED CONSOLIDATED COMPLAINT**
This document applies to: All Actions	Judge: Hon. Vince Chhabria Date: November 7, 2024 Time: 10:00 AM Ctrm: 4, 17th Floor

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES

Page(s)

Statutes and Codes

Other Authorities

Rules

I. INTRODUCTION

This case concerns Google's surveillance of Plaintiffs' and millions of other individuals' private activity on their Health Care Providers' websites. Using Google Analytics and other Google tracking technologies ("Google Source Code"), Google collected identifiable, intimate, and legally protected details about Plaintiffs' health, including the doctors they visited, treatment they received, and services they paid for.

This was not an accident or mistake. Not only was the Google Source Code purpose-built to intercept users' web activity—guaranteeing Google would receive identifiable health data if implemented on Health Care Provider web properties—but recently unsealed documents show that Google targeted Health Care Providers specifically, marketing its tracking technology to them as it sought to acquire more health data for use in "people-based" modeling, and advertising systems. This occurred despite Google's own recognition of the privacy and legal risks created by the incorporation of tracking technology on sensitive parts of providers' web properties; risks Google prevented providers themselves from understanding until the government acted in 2022.

Google's motion to dismiss overstates legal precedent and relies on fact-based challenges impermissible on a Rule 12 motion. No matter how much Google denies that it intercepts and uses Health Information, or claims it has policies proving a lack of "intent," its contradictory actions—and Plaintiffs' well-pled allegations about them—speak volumes. The Court should deny Google's motion in its entirety and allow this case to advance to discovery.

II. STATEMENT OF ISSUES TO BE DECIDED

Whether Plaintiffs adequately stated claims upon which relief can be granted.

III. PLAINTIFFS' FACTUAL ALLEGATIONS IN THE SAC

Plaintiffs' Second Amended Complaint (Dkt. 158, "SAC") provides clearer, factually-backed allegations that address each of the concerns in the Court's order dismissing the First Amended Complaint (Dkt. 86, "FAC").

A. Google Obtained Plaintiffs' Health Information

The Court previously found that the FAC's allegations regarding the "presence of source code" on Health Care Providers' web properties were insufficient to support that Google obtained

Plaintiffs' Health Information, given some judicially noticeable materials suggested Google Source Code could be configured to prevent the transmission of Health Information. *See* Dkt. 157. The following allegations address this issue.

1. Plaintiffs Are Patients Who Sought Health Care and Treatment

Plaintiffs are patients of six Health Care Providers who visited their provider's web properties for healthcare, treatment, and payment purposes. SAC ¶¶ 35-81. The SAC specifies why each Plaintiff visited their provider's web property, including the dates and actions taken. *Id*.

2. Google Source Code Tracked Plaintiffs Extensively

The SAC adds allegations connecting Plaintiffs' use of Health Care Provider web properties to Google's collection of health data by pleading that Google Source Code operated on sensitive subdomains where it plainly "doesn't belong" (Dkt. 157 at 6). Specifically, the SAC identifies Google Ads and Doubleclick Ads Code operating on sensitive subdomains for at least five of Plaintiffs' Health Care Providers, and Google Analytics Code for all six. SAC ¶¶ 39-42, 47-50, 55-57, 61-64, 68-70, 75-78. Plaintiffs further confirm the transmission of Health Information by pleading illustrative examples of data sent from "unauthenticated" webpages on their Health Care Provider web properties. *See id.*; SAC ¶¶ 34, 85, 88, 93, Exs. 1-2. This is consistent with research from the University of Illinois into Google Source Code (SAC ¶ 112, Ex. 4) which led the U.S. Department of Health and Human Services ("HHS") to update its Guidance about HIPAA compliance (*id.* ¶¶ 116, Exs. 6-7). In addition to these examples from "unauthenticated" webpages, the SAC alleges that all of Plaintiffs' providers, except Kaiser, used "authenticated" patient portals powered by Epic or Cerner, which also incorporated Google Source Code. SAC ¶¶ 37, 54, 60, 67, 72, 112, 115; *see*, *e.g., Doe I v. Medstar Health, Inc.*, No. 1:2023-cv-01198 (D. Md. May 5, 2023) Dkt. 37 at 3 (Cerner Opp. to Mot. for Prelim. Inj.) (Cerner acknowledging it used Google Analytics "to monitor user activity across its clients' [patient] portal domains").

3. The Information Google Collected Was Sensitive

The Court found that the FAC failed "to use precise language when describing the type of information that is allegedly transmitted." Dkt. 157 at 5 (discussing "[i]ndefinite language"). The

SAC addresses this concern with allegations detailing how Health Care Providers "are *actually* using Google's products." *Id.* at 6 (emphasis in original).

The SAC first defines "Health Information" consistent with FTC and HIPAA protections to include "identifiable" transmissions from both unauthenticated webpages and patient portals when patients visit them for purposes relating to "past, present, or future physical or mental health or condition; the provision of health care to [them]; or the past, present, or future payment for the provision of health care to [them]." SAC ¶ 21.

Next, the SAC explains how and why the information Google intercepted contained sensitive HIPAA-protected information. Paragraph 85 identifies and defines the technical terms associated with transmissions of the full-page URL (dl, url, or oref), the referring URL (dr or tiba), and other contents of transmissions, such as page titles and "events." The SAC demonstrates that Google Source Code transmits content information relating to upcoming procedures (SAC ¶ 40), medical services like "obsessive compulsive disorder" (*id.* ¶ 48), and from pages for specific medical providers (*id.* ¶ 62). *See also id.* ¶¶ 119-21 (examples on patient portal log-in pages, bill pages, services pages, and others), Ex. 2 at 1 (example transmission to Google with URL revealing page is for "urology" service), Ex. 2 at 6 (example transmission to Google with URL revealing page is for provider "emily-c-keadle-fnp-dnp"). Google also intercepted information showing when patients (including Plaintiffs) logged in to their patient portals, which conveys at least their status as a patient with that provider. *See, e.g., id.* ¶¶ 40, 48-50, 62-64; *see also id.* Ex. 2 at 2 (example transmission to Google with URL revealing "mychart-e-visit"). Google's Source Code *within* patient portals collects even more sensitive information. *See id.* Ex. 4 at 1 (testing of Google Analytics in patient portal revealed "Health Record: Blood Pressure"). Similarly, when patients use a provider's bill payment webpage (like Plaintiffs John Doe II and John Doe IV), Google intercepts Health Information reflecting past, present, or future payment for health care services. *See id.* ¶¶ 40, 48-49, 62, 70, 76; *see also id.* Ex. 2 at 4 (example of transmission to Google revealing patient is on Kaiser "consumer-sign-on" page and accessing the "bill[]pay" feature).

4. The Information Google Collected Was Identifiable

The SAC also precisely alleges how and why the information Google intercepted was

"identifiable" by demonstrating that one or more unique user identifiers accompany each transmission, and explains what data in the transmissions represent. SAC ¶¶ 90-109.

Notably, paragraph 97 defines specific identifiers—cid, gid, and auid—that Google obtains with other contents of Google Source Code transmissions, including identifiers that Google disguises as "first-party" cookies to evade attempts to avoid Google's tracking technology. SAC ¶¶ 24, 96-97; *see also* ¶ 93 (defining other cookies transmitted by Google Ads and Doubleclick Ads Code). Significantly, all six of Plaintiffs' provider web properties always transmitted values in the "cid" field which "uniquely distinguish all patients affected (including Plaintiffs) from other visitors to the same web property, and to Google specifically, within Google's systems." *Id.* ¶ 99; *see, e.g.,* Ex. 2. Thus, cid would accompany each Google Analytics transmission about Plaintiffs, and identify them. Ads, Doubleclick Ads, and Analytics Code also transmitted a "gid" for users signed into a Google browser at the time of the transmission (*id.* ¶ 96), while Ads and Doubleclick Ads transmitted the "auid" (*id.* ¶ 97). These were not the only identifying data Google acquired. Google also obtained users' IP addresses, which are personal identifiers themselves, with each transmission (*id.* ¶¶ 92, 102), in addition to classic third-party cookies in many instances (*e.g.* DSID, IDE, NID, Secure-3PSID) (*id.* ¶ 93). The data also includes identifiers for the Health Care Provider whose web property is affected, including a "gtm" value for their Google Tag Manager account, if they use the Google Tag. *See id.* ¶¶ 29, 169. The SAC further explains, as is evident from overlapping identifiers within transmissions (*see, e.g.,* SAC Exs. 1-2) that Google can and does commingle the data received at its Ads, Doubleclick Ads, and Analytics endpoints, including with other identifying information it maintains about a user. *See id.* ¶¶ 103-09.

B. Google's Conduct Was Intentional

The Court found that the FAC failed to plead that Google intended to collect Health Information, primarily because Google "warned" Health Care Providers not to "use its source code in ways that would result in HIPAA-covered information being sent to Google." Dkt. 157 at 7-8. The SAC corrects this deficiency by outlining a clear chronology of events, all of which indicate that Google's conduct was purposeful and for the purpose of serving Google's own interests.

1. Google Targeted Health Care Providers for Health Information

The SAC attaches a recently unsealed document from other litigation against Google (the "2017 Charter") showing that Google targeted Health Care Providers as a source of highly valuable user data and sought to increase their adoption of Google Analytics no later than 2017. *See* SAC Ex. 11; *id.* ¶¶ 4, 146-47. The 2017 Charter explains that Google's "objective" in targeting "healthcare" was to "grow…overall media measurement," and "secondarily" to "drive new…revenue." *Id.* It shows that Google evaluates the growth of "measurement," by several metrics, including "penetration in market" and "volume of data," supporting that Google intended to obtain *more* data from more Health Care Providers at an early time. SAC Ex. 11 at 263. The 2017 Charter also supports the allegation that Google specifically sought information about patients (Health Care Providers' "customers"): the "Integrations" product area within Google Analytics "ensures that [Google] has a comprehensive view of the customer journey & seamless way to take actions on these insights inside and outside of Google." *Id.* at 267; *see also* SAC ¶¶ 146-50 (explaining why Google knew and must have known that Health Care Providers would be incentivized to track patients, rather than non-customers, and encouraged the same). Along with the design of Google Source Code, this also supports Plaintiffs' allegation that Google intended to collect "identifiable" data: the "Analysis & Users" product area was focused on "pivot[ing] Google Analytics from sessions to people," and a "people-based data model" providing "user-based insights," which is inconsistent with any intent to collect only anonymized data. SAC Ex. 11 at 266. In short, the 2017 Charter shows that Google actively sought for at least *six years* to "grow" its access to Health Information maintained by Health Care Providers, including information belonging to Plaintiffs.

2. Google Did Not Warn Health Care Providers

Google succeeded in penetrating the healthcare industry and obtaining a higher volume of data. As the SAC shows, Google's Source Code reached near-ubiquity among Health Care Providers by 2023, appearing on more than 91% of over 5,000 Health Care Providers' web properties where it was generally present. SAC ¶¶ 111-15, 148, Exs. 1-2. Internally, the 2017 Charter acknowledged that there were "Privacy & Legal" risks associated with Google's plans to

provide a "single view of the customer" and gather "more comprehensive. . .data" through Google Analytics including through "inclu[sion]" and "analy[sis]" of data like "PII." SAC Ex. 11 at 269.

Google did not warn Health Care Providers about HIPAA violations that it knew were occurring as its source code proliferated across the health industry, nor did it update the Google Analytics Terms of Service to do so. Rather it posted a new help page, titled "Best practices to avoid sending Personally Identifiable Information (PII)." SAC ¶ 152. Although Google calls this its "HIPAA Policy[,]" in its briefing, any Health Care Provider who read this page would only have found a two-sentence "HIPAA Disclaimer" at the end which stated that Google did not intend to create HIPAA obligations *for itself*, and that HIPAA-covered entities "may not use Google Analytics" in ways "involving Protected Health Information [PHI]." *Id.*[1] This help page *did not* mention the identifiers (like cid) Google collected *by default*, which guaranteed the collection of PHI, and instead assured readers that "[t]o protect user privacy, Google policies mandate that no data be passed to Google that Google could use or recognize as personally identifiable information (PII)," misleadingly identifying several examples of potential "inadvertent[]" PII transmissions that users could control. *Id.* ¶ 157.

The Google Analytics Terms of Service, under the heading "Privacy," similarly stated: "You will not . . . pass information to Google that Google could use or recognize as personally identifiable information." *Id.* ¶ 156. The Google Analytics Terms of Service directed Health Care Providers, like all Google users, to Google's Privacy Policy for details on its data practices. *See id.* ¶ 131. The Privacy Policy, in turn, incorrectly claimed that Google does not collect a user's "Health Information" unless "you [users whose information is at stake] choose to provide it[.]" *Id.* at ¶ 181. These, and other similar, assurances—far from alerting providers to the guaranteed transmission of cid values and other identifiable data—gave the impression that Google Analytics only transmitted anonymous data by default. *See, e.g.,* SAC ¶¶ 152-60. If that were so, it would be safe for them to track their "customers" (patients) with Google's products, because only "identifiable" data is protected by HIPAA, which is what they did. *See* SAC ¶¶ 151-60.

[1] Google incorrectly characterizes RJN Exhibit 4, the 2018 version of this Help Page, as the "same HIPAA policy" it published in 2023. MTD at 13. In fact, it is only the minimized and downplayed HIPAA Disclaimer alleged in the SAC, with an additional sentence. *See* Pls.' Opp to RJN.

Google made no attempt to correct its policies, and issued no warning that using its products to track patients guaranteed HIPAA violations, for years after the 2017 Charter. It was not until March 2023, after *regulators* warned the industry about the use of Google Analytics, that Google posted an "Admonition" on its website. *Id.* ¶ 162. But even the Admonition did not disclose the actual, unavoidable, and material fact that Health Care Providers would transmit identifiable health data when tracking their "customers." *Id.* ¶ 164. Publicly available evidence to date overwhelmingly suggests that Google intended Health Care Providers to use its products as advertised and that they would not understand that doing so would result in Google intercepting Health Information. *Id.* ¶¶ 147, 152-61. Indeed, providers have been issuing health data breach notifications, in which they alerted patients that they only "recently learned" Google's source code caused the interception and disclosure of "certain patient information." *Id.* ¶ 161, n.86.

3. Google Used and Benefited from Obtaining Health Information

Google intended to collect Plaintiffs' Health Information because it served Google's interests to do so. Google unambiguously "admits to using 'information from sites or apps that use our services,' *i.e.* data obtained via Google Ads and Analytics, [including Plaintiffs,] in a variety of ways[]" (*id.* ¶ 129), and the SAC details available information about each admitted use (*id*. ¶¶ 123-44).

Any claim that Google's policies prevent it from using "sensitive" data it collects when Health Care Providers use Google services (consistent with its admissions) is belied by the policies themselves. By their literal terms, Google does not claim to exclude "sensitive" information from any "use," except one: "personalized" advertising. *See* SAC ¶¶ 130, 182. The SAC explains that "personalized" advertising is a "narrow subset" of the uses that Google admits to, and to the extent Google's personalized ads policies are enforced, such enforcement would primarily impact *providers'* use of the "people-based data model[s]" and "user-based insights," that Google creates from the data, not Google. *Id.* ¶¶ 130, 133-34, Ex. 11 at 266. Thus, Google's reliance on its use-related policy as evidence of lack of intent to obtain the data, falls short. Dkt. 164 ("MTD") at 13.

The SAC plausibly alleges that Google has not enforced prohibitions on the use of Health Information even in the context of personalized ads, because all of Plaintiffs' Health Care

Providers use Google Ads code on their web properties. *See, e.g.*, SAC ¶¶ 25, 40-41, 48-49, 55-56, 62-63, 68-69, 76-77, Exs. 1-2. And even if these providers had utilized Google's "controls" to limit Google's use of their patients' Health Information, that control would have been "ineffective." *Id.* ¶ 157; *see also id.* ¶ 135 (Google advising Analytics users that even when they turn "OFF" all of several default-enabled data sharing "controls," "data can still flow between Analytics and the other Google products [as relevant here, advertising products] that are explicitly linked to any of your account properties.").

IV. ARGUMENT

"At the pleading stage, all allegations of material fact are taken as true and construed in the light most favorable to the non-moving party." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir. 2020) (citation omitted). The facts alleged must "plausibly give rise to an entitlement to relief." *Id.* (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009)). A claim is facially plausible when the allegations allow for "the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 663 (citations omitted). Plaintiffs are to be "afforded the benefit of every favorable inference." *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 1014 (9th Cir. 2018). Defendants may not "exploit that benefit for themselves." *Id.*

A. Google Violated the Electronic Communications Privacy Act (ECPA)

The ECPA "is the primary law protecting the security and privacy of business and personal communications in the United States today." *Facebook Internet Tracking*, 956 F.3d at 598 (quoting S. Rep. No. 99-541, at 2 (1986)); *Joffe v. Google, Inc.*, 746 F.3d 920, 931 (9th Cir. 2013) ("paramount objective" is privacy) (citation omitted). A defendant violates the ECPA by (1) intentionally (2) intercepting (3) the contents of (4) an electronic communication (5) using a device. *See Facebook Internet Tracking*, 956 F.3d at 606; 18 U.S.C. §§ 2511(1)(a), 2520. One party's consent to the interception is a defense unless the interception was "for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Plaintiffs' ECPA claim is well pled.

1. Google Acted Intentionally Under 18 U.S.C. § 2511(1)(a)

Under the ECPA, "intentionally" means "purposefully and deliberately and not as a result

of accident or mistake." *U.S. v. Christensen*, 828 F.3d 763, 790-91 (9th Cir. 2015). In *Christensen*, an inventor who provided wiretapping software to a private investigation agency, which used it to conduct illegal wiretaps, argued he did not violate the ECPA because he believed the agency "was using his [] software for lawful purposes." *Id.* at 774, 790. In rejecting the argument, the Ninth Circuit held that "the operative question under [ECPA] is whether the defendant acted consciously and deliberately with the goal of intercepting wire communications." *Id.* at 775, 791.

The SAC meets the *Christensen* standard. Google does not dispute Plaintiffs' allegations that it acted deliberately with the goal of obtaining "wire communications." Nor could it. As in *Christensen*, Google deliberately distributed its wiretapping software to acquire "information concerning the substance, purport, or meaning" of electronic communications. 18 U.S.C. § 2510(4) (defining "intercept"), (8) (defining "contents"); SAC ¶ 24 (discussing design of Google Source Code), ¶ 170 ("Google made special efforts to ensure [transmissions]"), ¶ 242 ("Google targeted the healthcare industry to implement Google tracking technologies, knowing the use of the technologies on Health Care Provider web properties would transmit Health Information from patient visitors"), ¶ 244 ("actions were designed to learn or attempt to learn the contents").

Echoing the *Christensen* inventor, Google contends that Plaintiffs must plead that Google knew and "intended that healthcare providers use [its software] unlawfully to send Google PHI," and intended "that the healthcare industry violate Google's terms of service, policies, and federal law." MTD at 14 (*compare with Christensen*, 828 F.3d at 791 ("[defendant] contends that the word 'intentionally' [under the ECPA] must be read to require a defendant to know that his conduct is unlawful")). The Ninth Circuit rejected this exact argument, finding the "question of whether the defendant had a good or evil purpose in utilizing the [] recording equipment is [] irrelevant." *Christensen*, 828 F.3d at 775.

Even if Google's claims about the nature and purpose, and intended legality, of its interceptions could negate the element of intent, the defense is implausible here. The SAC alleges that Google not only did not fix, but also deliberately created, the "problem" of Health Information being intercepted. *In re Google Assistant Priv. Litig.*, 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020) (inferring intent where defendants "ha[d] not fixed the problem" of known interceptions); SAC ¶

145. At the very least, Google knew and must have known that unlawful interceptions "might be" occurring. *Abraham v. Cnty. of Greenville, S.C.*, 237 F.3d 386, 392 (4th Cir. 2001); *see, e.g.,* SAC ¶¶ 170-73. Meanwhile, Google pursued expansion in the healthcare industry where the significant "value" of its Source Code (to Health Care Providers) lay in tracking the Health Information Google claims it did not want to—but did—receive. *See, e.g.,* SAC ¶¶ 148, 162; SAC Exs. 1-2; *U.S. v. Hugh*, 533 F.3d 910, 912 (8th Cir. 2008) (intent established by, among other things, evidence of recordings in defendant's possession). That Google benefited from increasing its "overall media measurement" of healthcare, and driving new revenue, as well as fueling advertising and other Google products, only makes it more plausible that Google's receipt of Health Information was not an "accident or mistake." SAC ¶¶ 146, 149; *In re Pharmatrak, Inc.*, 329 F.3d 9, 23 (1st Cir. 2003) ("[a]n interception may be more likely to be intentional when it serves a party's self-interest to engage in such conduct").

Google's claim that its HIPAA Disclaimer was a meaningful warning only confirms that the policies it relies upon were *intended* to do no more than provide a modicum of deniability for Google, whose protests demonstrate "willful blindness" under the most generous interpretation of the facts alleged. *Global-Tech Appliances, Inc. v. SEB, S.A.*, 563 U.S. 754, 766-70 (2011).

2. Google Does Not Establish Consent Under 18 U.S.C. § 2511(2)(d)

Plaintiffs allege that neither they, nor their Health Care Providers, consented to Google intercepting Plaintiffs' Health Information. *See, e.g.,* SAC ¶¶ 81, 161, 174, 218-21. Google never addresses the allegations about Health Information. Rather, it contends that Health Care Providers "consented to the use of Google's products by choosing to incorporate the source code on their Websites." MTD at 14-15. This general consent to the "use" of its technology, Google claims, is sufficient to establish consent to the interception of Health information. *Id*. This is wrong.

The consent defense applies only if "one of the parties to *the* communication has given prior consent to *such* interception." 18 U.S.C. § 2511(2)(d) (emphasis added). This requires Google to "explicitly notify users of the conduct at issue"— the collection of Health Information— as "consent is only effective . . . to the particular conduct, or to substantially the same conduct" that was disclosed. *Calhoun v. Google, LLC*, 2024 WL 3869446, at *5 (9th Cir. Aug. 20, 2024)

(citations and quotation marks omitted). Google bears the burden of proof on its affirmative defense.

As in *Calhoun*, whether Healthcare Providers consented to use Google Source Code, generally, does not end the inquiry. What matters, under "the circumstances, considered as a whole," is whether Google "explicitly notif[ied] users of the conduct at issue"—i.e., the collection of patient Health Information—and they agreed to it. *Calhoun*, 2024 WL 3869446 at *5. Google does not carry its burden on this. Plaintiffs allege that Health Care Providers did not consent because: (1) they are legally obligated to secure identifiable health information (SAC ¶¶ 175-77, 220); (2) Google's uniform policy documents omitted and obscured that transmissions were identifiable (*id.* ¶¶ 145-60, 221); and (3) providers issued breach notifications expressing they did not know unlawful transmissions to Google would occur (*id.* ¶ 161). Indeed, providers cannot "consent" to disclose Health Information without "express written authorization," rendering Google's claim based on "use" of its tracking technologies unlawful and implausible. SAC ¶ 220.

These allegations satisfy applicable pleading requirements. They concern principles of statutory and contract interpretation, and need not satisfy Rule 9(b). *See Smith v. Google, LLC*, 2024 WL 2808270, at *5 (N.D. Cal. June 3, 2024) (rejecting argument that intent allegations trigger Rule 9(b)). Nonetheless, Plaintiffs respond to Google's affirmative defense with specificity. As set forth above, and in the SAC, Google (who) successfully marketed Google Ads, Doubleclick Ads, and Analytics Code to Plaintiffs' Health Care Providers (what) by downplaying and obscuring the truth that using those products as advertised, to track providers' "customers," would result in HIPAA violations by sending identifiable transmissions to Google (how) in the Google Analytics Terms of Service and other policy documents (where) throughout the time each version of each document was posted to Google's website (when) because Google wanted access to data available to Health Care Providers, secondarily generating additional revenues, and Google benefited significantly from obtaining Health Information (why).

3. Any Consent Is Invalid Under 18 U.S.C. § 2511(2)(d)

Even if Google were correct that Health Care Providers' consent to "use Google's products" encompassed Health Information, that consent was procured by false pretenses,

omission, or known mistake, rendering it invalid. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004); *Desnick v. ABC*, 44 F.3d 1345, 1351 (7th Cir. 1995). Health Care Providers agreed to use the products due to omissions in Google's disclosures, and, as evidenced by widespread use of the source code on sensitive webpages, any consent was provided under the mistaken belief (known to, and encouraged by, Google) that patient communications on sensitive webpages could be tracked without compromising protected information. *See* SAC ¶¶ 145-60, 221, 223.

Google's defense thus fails for the additional reason that consent of "one of the parties to the communication" is ineffective if "such communication is intercepted for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). "[T]he focus . . . is upon whether the *purpose* for the interception—its intended use—was criminal or tortious." *U.S. v. McTiernan*, 695 F.3d 882, 889 (9th Cir. 2012). No partially "lawful purpose" can "sanitize" an interception "made for an illegitimate purpose." *Sussman v. ABC*, 186 F.3d 1200, 1202 (9th Cir. 1999).

Google acquired Plaintiffs' Health Information for criminal and tortious purposes, including to invade their privacy and in criminal violation of HIPAA regulations. *See* SAC ¶ 222. This is sufficient to invalidate any Health Care Provider's consent. *See In re BetterHelp, Inc. Data Disclosure Cases*, 2024 WL 3416511, at *4 (N.D. Cal. July 15, 2024) (claims that "implicate[d] HIPAA, . . . sufficient"); *Mekhail v. N. Mem'l Health Care*, 2024 WL 1332260, at *5 (D. Minn. Mar. 28, 2024) (similar allegations sufficient); *Cooper v. Mount Sinai Health Sys., Inc.*, 2024 WL 3586357, at *9 (S.D.N.Y. July 30, 2024) (same). Google claims its purpose was only "to make money" (MTD at 17), but this provision looks to the "purpose" of the interceptions, not defendant's "motive." *Kurowski v. Rush Sys. for Health*, 2024 WL 3455020, at *5 (N.D. Ill. July 18, 2024). "Many crimes and torts are motivated by a desire to make money, and 'it defies common sense that a clearly harmful act could escape liability as long as it was done for profit.'" *Id.*; *Cooper*, 2024 WL 3586357 at *9 ("theory that the presence of a primary financial motive inoculates a defendant from liability under the ECPA is wrong"). Google's assertions regarding its "purpose" also contradict the facts alleged. The 2017 Charter shows that "revenues" were a *secondary* purpose for Google, behind gaining (unlawful) access to "healthcare" data. Google's invasive and offensive uses of Health Information are yet another tortious purpose for intercepting it. *See* SAC

¶¶ 123-44; *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1068 (N.D. Cal. 2021) ("purpose of [interception was to] associat[e] [] data with user profiles" which is "criminal or tortious").

Plaintiffs also allege that if Google were correct about Health Care Provider consent to the interceptions (which Plaintiffs dispute), such consent was also for criminal and tortious purposes. *See* SAC ¶ 224. More specifically, Google claims that it intercepted communications at Health Care Providers' direction. *See e.g.*, MTD at 18. As discussed above, if that were true, it would mean providers used Google Source Code for the purpose of effectuating "the particular conduct" alleged, such that they violated Section 2511(1)(a) *with* Google, by "procur[ing] any other person to intercept" Health Information. If Health Care Providers "procure[d]" Google, then their consent to the interceptions would not insulate Google, because *their* purpose for the interceptions was also criminal and tortious—i.e., disclosing Health Information in violation of state and federal law.

Google's argument that the "exception [only] asks what the interceptor's purpose was" misreads the ECPA and ignores its legislative history. MTD at 17. The ECPA originally exempted *any* interception where one party consented. This was rejected for possibly allowing one party to wiretap for "insidious purposes," including by "consent[ing] to the use of an electronic device by a nonparty" to the communication. Act of Apr. 29, 1968, Pub. L. No. 90-351, 1969 U.S.C.C.A.N. 2112, 2236. The result was a narrower consent exemption, enacted as Section 2511(2)(d), that renders consent invalid if the communication is intercepted for an interceptor's *or* the consenting party's insidious purposes. *See Moore v. Telfon Commc'ns Corp.*, 589 F.2d 959, 966 n.3 (9th Cir. 1978).

B. Google Violated the California Invasion of Privacy Act (CIPA)

Plaintiffs allege that Google violated CIPA by "read[ing], or attempt[ing] to read, or to learn" the "contents" of communications, "willfully and without the consent of all parties to the communication, or in any unauthorized manner." Cal. Penal Code § 631(a); SAC Count Two. Plaintiffs also allege Google violated Section 632 by intentionally recording communications "carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties." SAC ¶ 237. Google disputes Plaintiffs' allegations of scienter under both provisions. It also contends that it acted lawfully as a "vendor" under Section

631, and that none of the information it learned from Plaintiffs' communications constituted "contents." Google further denies "record[ing]" communications under Section 632 and asserts that Plaintiffs' communications were not "confidential." MTD at 18-20.

1. Google Acted Willfully, in Unauthorized Ways, and Intentionally

Similar to the ECPA, the word "willfully" in Section 631 means not "inadvertent." *People v. Buchanan*, 26 Cal. App. 3d 274, 287 (1972). Plaintiffs' allegations that Google read and learned the contents of their communications by design, are sufficient. *See supra* § III.A. "While Google argues that judicially noticeable policy documents suggest that Google did not actually want to receive personally identifiable information and expressly prohibited developers from transmitting such data, this presents a question of fact that the Court cannot resolve at this stage." *Smith v. Google, LLC*, 2024 WL 2808270 at *5.

2. Google Is Not an Extension of Health Care Providers

Section 631 prohibits the "simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device." *Ribas v. Clark*, 38 Cal. 3d 355, 360-61 (1985). In recent years, defendants have sought to distinguish themselves from "unannounced second auditors," who are subject to liability, by characterizing themselves are mere "vendors," who allegedly are not. *See Rodriguez v. Ford Motor Co.*, 2024 WL 1223485, at *9-14 (S.D. Cal. Mar. 21, 2024) (describing state of the law). For courts that have considered this distinction, the analysis turns on whether the defendant has the "capability" to use the information it learns for its own purposes; an auditor does, while a vendor does not. *See e.g.*, *Smith v. Google, LLC*, 2024 WL 2808270 at *4 (sufficient that "'Google Analytics…is not simply a 'tool' utilized by website owners for their own purposes' but that Google 'benefits (and profits from)' the use of Google Analytics and 'can use the data'"); *Price v. Carnival Corp.*, 2024 WL 221437, at *3 (S.D. Cal. Jan. 19, 2024) (no "exception" for entity that allegedly processed data "to generate analytics").

While the Court should reject Google's argument because there is no "vendor" exception in CIPA, Google cannot qualify as a "vendor" because the SAC plausibly alleges that it not only has the "capability" to but, in fact, uses the Health Information it intercepts, for its own purposes. *See supra* § III.B.3 (describing Google's uses and reservation of rights to use the information).

Google refuses to confront this obvious distinction between its own conduct and the passive tools described in *Graham v. Noom*, 533 F. Supp. 3d 823 (N.D. Cal. 2021), and other early cases addressing vendors. Instead, Google argues it is a vendor because Health Care Providers can "control whether and how Google processes their data." MTD at 18. But whether some potential for control existed is not the inquiry, particularly where, as here, the allegation is that providers did not even know the conduct needed to be controlled. "The key is whether the hiring of a third party to collect information–even if for the benefit of the contracting party–poses a materially enhanced risk to the individual's privacy." *Doe v. Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *17 (N.D. Cal. Apr. 11, 2024). Google's argument about controls also disputes the facts alleged. *See, e.g.*, SAC ¶ 31 ("Google maintains sole control over the code"), ¶ 135 ("settings do not control interceptions via Google Ads Code and Google's associated uses"), ¶¶ 157-58 (settings are "ineffective" and Google does not disclose true level of control).

3. Google Read and Learned "Contents" of Protected Communications

Google's suggestion that it obtains only meaningless "record information" rather than "contents" (MTD at 19), ignores Plaintiffs' allegations of substantive transmissions. *See, e.g.*, SAC ¶¶ 25-78, 85-89, 119-21, Exs. 1-2. This Court previously questioned whether the contents of Plaintiffs' private health information were even at issue because Plaintiffs did "not adequately allege where on a web property the source code actually exists." Dkt. 157 at 12-13. The SAC cured that deficiency. *Supra* § III.A.

Under CIPA, "any information relating to the substance, purport, or meaning" of a communication qualifies as "contents." *In re Google RTB Consumer Priv. Litig.*, 606 F. Supp. 3d 935, 949 (N.D. Cal. 2022) (same as ECPA). URLs and other data from web browsing activity meet this definition when they convey substantive information, as alleged here. *See, e.g. Facebook Internet Tracking*, 956 F.3d at 596, 605 (concluding URLs that could disclose search terms were "contents," in part because they could divulge "a user's personal interests, queries, and habits"); *In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 137 (3d Cir. 2015); *Doe v. Meta Platforms, Inc.*, 690 F. Supp. 3d 1064, 1076 (N.D. Cal. 2023) (patient portal logins and descriptive health URLs); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 935-36 (N.D. Cal. 2023).

Here, URLs disclosing searches for medical professionals specific to a plaintiff's medical needs, communications about bill payments, scheduling appointments, and specific conditions, which Google allegedly obtained, meet the definition of content. *See, e.g.*, SAC ¶¶ 35-78, 85-89, 119-21.

Google's argument to the contrary overstates its authority. The court in *Doe v. Cedars-Sinai Health Sys.*, 2024 WL 3303516 (Cal. Super. June 5, 2024)[2] did not "hold[]" that "pages the patient clicked on and doctors'[sic] names" are not "contents" as a matter of law. On the contrary, it recognized that "'descriptive URLs' that include the path and a query string with detailed information about the search contain 'the substance of a communication,'" and that courts have held allegations about "personal search queries - such as specialty healthcare providers and treatments for medical conditions" could plausibly allege "contents," but found the Plaintiffs in that case did not make the necessary allegations. *Id.* at *2-3. Google's reliance on *Jones v. Peloton Interactive, Inc.* is similarly misplaced. The *Jones* plaintiffs alleged that defendant obtained "the full transcript of the conversation" at issue but did "not identify enough facts about the content." 2024 WL 1123237, at 4 (S.D. Cal. Mar. 12, 2024). Lastly, Google's Ninth Circuit authority, *In re Zynga Priv. Litig.*, only stands for the proposition that not all data necessarily constitutes "contents," not that Plaintiffs failed to allege "contents" here. 750 F.3d 1098 (9th Cir. 2014).

4. Google Recorded Confidential Communication Under Section 632

Google argues that Section 632 does not apply because "Google did not 'record' the data transmitted; rather, the Websites [did]." MTD at 19. Not only does Google cite no authority for this claim, but these types of counter-factual arguments contesting Plaintiffs' well-pled allegations that Google recorded patient data are improper at the pleading stage. *See Gladstone v. Amazon Web Servs., Inc.*, 2024 WL 3276490, at *9 (W.D. Wash. July 2, 2024) (rejecting argument at pleadings stage that defendant's customer, and not defendant, actually "uses" and "record[s]"); *Doe v. FullStory, Inc.*, 2024 WL 188101, at *8 (N.D. Cal. Jan. 17, 2024) (same).

[2] The MTD's citation to this case, an unpublished California Superior Court case, violates Rule 8.1115 of the California Rules of Court which forbids citation of unpublished California opinions except in certain circumstances not relevant here.

Next, Google claims the Health Information at issue is not confidential because "Google instructed the Websites to disclose the use of Google Analytics; post a privacy policy, and obtain consent where required by law" such that "Plaintiffs do not have a reasonable expectation of privacy in their analytics data." MTD at 20. This consent-based argument fails. *First*, the documents Google cites have nothing to do with what was disclosed to *Plaintiffs*, but reflect general, developer documentation *Id*. *Second*, even if Health Care Providers did, generally, maintain privacy policies, the mere existence of such generalized documents does not establish that they contained clear and adequate disclosures that would be sufficient to rebut Plaintiffs' established expectation of privacy in their own health data or to obtain legally valid consent, which must be specific. *See Smith v. Google, LLC*, 2024 WL 2808270 at *3 ("mere existence of various terms of service and privacy policies cannot establish at [pleadings] stage . . . that any of the plaintiffs *did* in fact consent."); *Brown v. Google LLC*, 525 F. Supp. 3d at 1063 (consent "must be actual" and "the disclosures must 'explicitly notify' users of the practice at issue").

Cedars-Sinai does not advance Google's position. There, plaintiffs sued their hospital, alleging that the hospital recorded their "confidential" communications on the hospital websites in violation of Section 632. The Court rejected this argument because (1) the plaintiffs had already consented to the hospital accessing their "personal medical information" and (2) a person generally "expect[s] the website owner" to "record" the actions taken on their website. *Cedars-Sinai*, 2024 WL 3303516 at *4. By contrast, Google has not established Plaintiffs ever consented to Google recording their communications with Health Care Providers, and Google promised *not* to collect Health Information unless Plaintiffs chose to provide it. *See infra* § IV.D.

C. Google Violated Plaintiffs' Constitutional and Common Law Privacy Rights

A claim under the California Constitution's right to privacy requires: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) conduct by the defendant that amounts to a serious invasion of the protected privacy interest. *Hill v Nat. Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994). A common law intrusion claim requires: "(1) intrusion into a private place, conversation or matter, (2) in a manner highly offensive to a reasonable person." *Shulman v. Grp. W Prods., Inc*., 18 Cal. 4th 200, 231 (1998). Google disputes

that: (1) Google intended to intrude, (2) Plaintiffs had a reasonable expectation of privacy in the data transmitted, and (3) the intrusions occurred in a highly offensive manner. *See* MTD at 20-22.

A defendant's intent is evaluated as one of "the surrounding circumstances" that determines whether an alleged intrusion is serious and highly offensive. *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 295 (2009). Google's conduct is offensive in many ways. *See, e.g.*, SAC ¶ 81 (Plaintiffs did not consent), ¶¶ 163, 175, 262 (tracking inappropriate in context), ¶ 181 (Google promised not to collect "health information" unless users chose), ¶ 182 (Google gave the impression that health information would not be used), ¶¶ 184, 267-70 (Google disguised third-party cookies to evade privacy controls), ¶ 185 (conduct causes "medical mistrust"), ¶ 256 (conduct violated provider-patient confidentiality and applicable laws). That Google acted on purpose, to benefit itself financially and by securing valuable sensitive data, is one of many offensive characteristics supporting Plaintiffs' claims. *See id.* ¶¶ 123-44, 187 (intrusion was self-serving), ¶¶ 145-73 (intrusion was knowing, and intentional); *see also supra* § III.B. The Court's decision in *Caraccioli v. Facebook, Inc.* (MTD at 20-21) not to credit a *pro se* plaintiff's argument that Facebook "published" defamatory content in violation of publicity rights, where Facebook's Terms of Service disclaimed publishing, does not support Google's argument that its policy documents rebut Plaintiffs' allegations here. 167 F. Supp. 3d 1056 (N.D. Cal. 2016).

As for whether Plaintiffs' expectation of privacy was reasonable, of course Plaintiffs have a reasonable expectation of privacy in their *Health* Information. *See* SAC ¶¶ 174-85; *In re Meta Healthcare Pixel Litig.*, 647 F. Supp. 3d 778, 801 (N.D. Cal. 2022) (defendant did not cite "a single case where a court found that the collection of the kinds of [health] information at issue here did not constitute a highly offensive invasion of privacy"); *Katz-Lacabe v. Oracle Am., Inc.*, 668 F. Supp. 3d 928, 942 (N.D. Cal. 2023) (collection of health information supported claims).

Google's argument that receiving the intensely revealing types of URLs and data shown in SAC Exhibits 1 and 2 is HIPAA-compliant misunderstands that statute, and case law interpreting it. The out of context snippets from *Am. Hosp. Ass'n v. Becerra,* on which Google relies, only reflect that HHS lacks authority to directly prohibit all tracking on webpages relating to health. This is because it is possible *some* of the visitors are not patients, such that transmissions would

not *always* contain Health Information—but the obligation to prevent the transmissions would *always* be enforceable under the rule vacated in that case. This is irrelevant because Plaintiffs are patients of their respective Health Care Providers and bring this action regarding transmissions of information about visits relating to their healthcare, which HHS, and all parties, and the Court in *Am. Hosp. Ass'n*, among others, agree is Health Information. *See* RJN Ex. 10; *Am. Hosp. Ass'n v. Becerra*, 2024 WL 3075865, at *13 (N.D. Tex. June 20, 2024); SAC ¶ 117; *supra* § III.A. In addition, Google ignores that the FTC defines "health information" to mean "anything that conveys information that enables an inference about a consumer's health." SAC ¶ 21.

Google relies on the holding in *Smith v. Facebook*, 745 F. App'x 8, 9 (9th Cir. 2018), that certain transmissions via Facebook's "Like" button were not actionable because Facebook's terms of service disclosed them, and dicta in *Cousin v. Sharp Healthcare*, 681 F. Supp. 3d 1117, 1123 (S.D. Cal. 2023), about how *Smith* might have applied to different allegations. *See* MTD at 21. But "[t]his case is different than *Smith*" for the same reasons Judge Orrick distinguished it in *In re Meta Healthcare Pixel Litig.*, 2024 WL 333883, at *2 (N.D. Cal. Jan. 29, 2024) (this tracking "captures information that connects a particular user to a particular healthcare provider"). It is also distinguishable because Google's terms of service said it would *not* collect "health information" without further action by Plaintiffs (*see* SAC ¶¶ 181-82), yet Google engaged in extensive tracking, even on patient portals. *See supra* § III.A.2.

Google's other arguments about offensiveness—(1) that HHS said "tracking technologies are common[]"; (2) that Plaintiffs do not allege receiving advertisements; and (3) that, according to Google, Plaintiffs only plead HIPAA-compliant tracking (MTD at 22)—do not support dismissal. *First*, the proliferation of Google Source Code on Health Care Provider web-properties is a nationwide privacy problem that only recently gained public attention, not a defense. SAC ¶¶ 111-13. *Second*, none of Plaintiffs' claims are based on receiving advertisements; Plaintiffs allege Google uses their Health Information for many purposes that would not result in "personalized advertising"—what is offensive is that Google does "far more with the information than store it." SAC ¶ 123. Plaintiffs also demonstrate that their Health Care Providers' Google Analytics accounts were linked to Google Ads Code, as Google encourages, such that Plaintiffs' data flows

into Google's advertising systems, even *if*, as it claims, Google prohibits providers from running advertising campaigns with it themselves. SAC ¶¶ 25, 27, 124, 133, Exs. 1-2. *Third*, whether *some* "tracking technologies" can be used in compliance with HIPAA is beside the point given the SAC's clear allegations that Google's Source Code was not.

Google's reliance on *Doe v. Kaiser Found. Health Plan, Inc.*, 2024 WL 1589982, at *19 incorrectly portrays a ruling regarding inadequate factual allegations as a ruling of law. While *Kaiser* did dismiss an intrusion claim which was based in part on Google's conduct alleged here, it did so because "there [were] no allegations that Kaiser *knew and/or approved* of third parties collecting and/or using information for their own purposes." *Id.* (emphasis added). Kaiser's knowledge, and the offensiveness of *Kaiser's* conduct, were poorly pled in that case. Here, Plaintiffs' allegations of Google's knowledge and intent are robust. *Supra* § III.B. *Kaiser* only supports the allegations that Health Care Providers did not actually consent.

D. Google Breached its Contract of Adhesion with Account Holders

Plaintiffs predicate their breach of contract claim on applicable terms in Google policy webpages set forth in the SAC. *See* SAC ¶¶ 275-92, Exs. 9, 14, 15 (TOS, Privacy Policy, Personalized Advertising); *Brown v. Google LLC*, 2021 WL 6064009, at *10 (N.D. Cal. Dec. 22, 2021) (noting contract need only "guide" parties to incorporated documents).

The first alleged breach involves Google's promise to collect only health information that users choose to provide. *See* SAC ¶¶ 285-86. The Privacy Policy contains a section titled "Categories of information we collect" and one of the categories is "Health information," which Google says is collected only "if you choose to provide it." SAC ¶ 181, n.97, Ex. 14 at 17-18. Everything about this provision creates the reasonable expectation of an "opt-in" environment for a special category of information, from the statement "*if you choose*" to Google's illustration of data collected when users affirmatively deploy Google's "health-related features." *Id.*

Google's argument that this provision of its uniform Privacy Policy only "applies" to users who *do* deploy Google's "health-related features" ignores the structure of the contract. *See* MTD at 22-23. "Health Information," with the caveats discussed above, appears as one category of information Google is legally obligated to disclose that it collects, under the larger heading "U.S.

state law requirements." Ex. 14 at 16. A reasonable user would understand from the structure, and the text, that Google's description of the "Health Information" it collects is accurate and robust: if they opt into Google's health-related features, information relating to their physical and mental health will be collected; if they decline to opt in, it will not be collected. Ninth Circuit law does not permit Google to redefine ordinary terms like "Health Information" to escape what the language and structure of its policies would tell an ordinary person using standard definitions. *See Calhoun*, 2024 WL 3869446, at *9 ("reasonable" user is not "someone who is able to easily ferret through a labyrinth of legal jargon"); *see also* SAC ¶ 21 (explaining what "Health Information" is); *Meta Healthcare Pixel,* 647 F. Supp. 3d at 792 (applying ordinary definition). Unlike the FAC, the SAC shows that the information Google collected contains Health Information (*supra* § III.A), which, contrary to Google's promise, Plaintiffs did not "choose to provide" to Google. *See* SAC ¶ 286.

Google attempts to confuse the issue by pointing to a different provision in its policies covering "Internet, network, and other activity information" (MTD at 23), but the "specific" terms at issue, regarding Health Information, "control over general ones." *S. Cal. Gas Co. v. City of Santa Ana*, 336 F.3d 885, 891 (9th Cir. 2003). Even if Google's interpretation created an ambiguity, that should be resolved in Plaintiffs' favor. *See Daniel v. Ford Motor Co.*, 806 F.3d 1217, 1224 (9th Cir. 2015); *Khoja*, 899 F.3d at 1014. Google cites no authority holding otherwise. *Kurowski* upheld plaintiffs' breach of contract claim, even though the court determined that the data alleged did not "fit" the legal definition of individually identifiable health information under HIPAA, because – consistent with the allegations here ("information relating to … health") – the contractual definition was broader. 2023 WL 4707184 at *4. In *Smith v. Facebook*, the court evaluated whether the plaintiffs "consented" to certain tracking based on Facebook's policy provisions; the policies at issue contained no promises relating to "health information" so there were no ambiguities or fact disputes to resolve, the putative class was not limited to patients, and the healthcare websites were not limited to covered entities. 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017).

The second alleged breach involves Google's promise not to use Health Information for "personalized ads." *See* SAC ¶¶ 287-91. Google acknowledges several times in its Privacy Policy that information relating to health is "sensitive." Ex. 14 at 6, 23, 30. Google's statements about its use of sensitive information in personalized ads, which are also prevalent throughout Google's policies and incorporated documents, give the impression that Google walls Health Information off from any potentially offensive use, and will not use sensitive data to "target[]" users or fuel its advertising business. In reality, Google relies on an artificially narrow reading of "personalized ads" that does not recognize the sensitivity of this information, and does not comport with how a reasonable user would understand Google's policies relating to its use of Health Information.

In the context here, the meaning of Google's promise is that Google will avoid any personalized or advertising use outside the scope of the service being offered to the Health Care Provider that installed Google Source Code. *See* SAC ¶¶ 289-90. In Google's own private language, by contrast, "personalized advertising" only means creating "audiences" for advertisers to target, either through "remarketing" to their own customers, or by selecting a Google-curated audience. SAC ¶¶ 130, 133-34, Ex. 15 at 4 (describing "effect of the policy"). Google's "personalized ads" policies thus do not (despite the impression) encompass other "personalized" uses of Health Information that Google admits to, such as "content" or any other targeting. *See id.* Similarly, the policies do not encompass Google's "advertising" machinery generally, including uses to train Google's advertising AI, measure the effectiveness of advertising, target websites likely to have particular types of users, for advertising placements, or for any other use in support of Google's advertising business. *See id.* ¶¶ 132-33, 135-44. Google's internal nomenclature allows Google to simultaneously admit to a host of "uses" of Health Information that an ordinary person would not readily consent to, while giving the distinct impression that, as Google suggests in its motion to dismiss, "Google explains that it 'will never use sensitive information like health[.]'" MTD at 11 *but see* RJN Ex. 5 at 4 (statement is limited to "to tailor ads to users.").

Google's defense relies heavily on the fact that Plaintiffs do not plead a specific personalized ad they received. *See* MTD at 10, 17, 22. Even if that exclusion could support an inference that Google actually enforced its "personalized ads" policy, it would have no bearing on

the other uses that Google admits to and for which it has no policy against using sensitive data. Google's contention that Plaintiffs have not alleged receiving personalized "content" (MTD at 12, 22) ignores the distinction: unlike personalized "ads," Google does not even claim to have a policy against using Health Information for personalized "content." It would turn Rule 12(b) on its head to require Plaintiffs to plead not only the defendant's unambiguous admission, but also evidence to refute that the defendant enforces a policy it does not, and cannot, claim to have.

Google's breach of contract invaded Plaintiffs' privacy, deprived them of the benefit of their take-it-or-leave-it bargain with Google, and enriched Google, including by providing data to improve and "personalize" Google's products and services. *See* SAC ¶ 292. Google argues that Plaintiffs are unable to show damages, but it relies on the assumption that Plaintiffs failed to plead Health Information was transmitted. MTD at 24. Plaintiffs have set forth specific allegations of how Google breached its promises to Plaintiffs and the harm that flowed. *See* SAC ¶ 292. On the law, Plaintiffs can seek damages for "the detriment caused by the breach." *Stephens v. City of Vista*, 994 F.2d 650, 657 (9th Cir. 1993). "[T]he failure to perform a duty required by contract is a legal wrong, independently of actual damage sustained by the party to whom performance is due." *In re Google Referrer Header Priv. Litig.*, 465 F. Supp. 3d 999, 1010 (N.D. Cal. 2020); *see also Tribeca Cos., LLC v. First Am. Title Ins. Co.*, 239 Cal. App. 4th 1088, 1103 n.12 (2015) (plaintiff who successfully demonstrates breach of duty, such as breach of contract, but cannot show actual damages or "appreciable detriment," still entitled to recover nominal damages); Cal. Civ. Code § 3360 ("When a breach of duty has caused no appreciable detriment to the party affected, he may yet recover nominal damages.").

E. Google Breached the Implied Covenant of Good Faith and Fair Dealing

Contracts impose a "duty of good faith and fair dealing[,]" *Chauhan v. Google LLC*, 2023 WL 5004078, at *3 (N.D. Cal. Aug. 4, 2023), which obligates parties to do nothing '"which injures the right of the other to receive the benefits of the agreement.'" *Olyaie v. Gen. Elec. Cap. Bus. Asset Funding Corp.*, 217 F. App'x 606, 611 (9th Cir. 2007) (citation omitted). Evading "the spirit of the bargain" and "abuse of a power to specify terms" are actionable. *Id.*

The SAC alleges Google violated the implied covenant by drafting and selectively interpreting the terms "health information," "identifiable," and "personalized advertising" in a manner inconsistent with how any reasonable person would view them. *See* SAC Count Six. Google's unreasonable construction of these terms deprived Plaintiffs of the benefit of the bargain with respect to promised transparency and control of their information. *See id.* ¶¶ 296-97.

Specifically, and contrary to Google's interpretations: (1) it is reasonable to read the term "health information" to encompass the Health Information at issue here, that is: "medical history….and other similar information related to your physical or mental health" (*id*. ¶ 181); (2) if Health Information is collected, it is reasonable to read Google's promises to include a covenant to *not* use it except in service to Health Care Providers who used Google services (*id.* ¶ 182); and (3) it is reasonable to read Google's promises to include a covenant that users (whether Plaintiffs or providers) are in control of "identifiable" information (*id.* ¶¶ 158-59). In whole, any reasonable interpretation of these provisions concludes Google neither collects nor uses Health Information without Plaintiffs' and Health Care Providers' knowledge and consent. Yet in practice, Google does exactly that. And, in order to legitimize its conduct, Google seeks to assert a strained interpretation of these terms by: (1) asserting that "health information" only includes data transmitted through health-related Google services; (2) asserting that "personalized *ads*" *excludes advertising* via remarketing, conversion tracking, and targeting contextual advertising as well as other personalization; and (3) defining "identifiable" information to exclude recognized identifiers, like IP addresses and cookie values. *See id*. ¶ 297. Google's interpretations are unreasonable given the terms' plain meanings, state and federal laws, and Google's own policies (*see, e.g.*, *id.* ¶¶ 90, 134, n.54, 181). Google's acts evade the spirit of the bargain, and frustrate Plaintiffs' rights to contractual benefits, including the ability to understand what, where, and how Google collects data, and what Google does with it.

F. Google Was Unjustly Enriched at Plaintiffs' Expense

The SAC alleges unlawful conduct by Google which enriched it through the collection, use, and monetization of Health Information (*see* SAC ¶¶ 300-11), thereby entitling Plaintiffs to seek restitution and disgorgement of Google's wrongful gains. Accordingly, the Court may

construe the claim as a quasi-contract cause of action. *See Astiana v. Hain Celestial Grp., Inc*., 783 F.3d 753, 762 (9th Cir. 2015). Further, and contrary to Google's contention, Plaintiffs can plead both express contract and unjust enrichment in the alternative. *See id.*; *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019) (plaintiffs may plead breach of contract and unjust enrichment as alternate claims); Fed. R. Civ. P. 8(d)(2)-(3).

V. CONCLUSION

For the reasons set forth above, Plaintiffs respectfully request that the Court deny Google's Motion. In the alternative, recognizing that the Court has previously indicated that this SAC may be Plaintiffs' last opportunity, in the event some aspect of the SAC is inadequate, Plaintiffs nonetheless respectfully request that the Court grant further leave to amend.

Dated: September 17, 2024

SIMMONS HANLY CONROY LLC

/s/ Jay Barnes
Jason 'Jay' Barnes

Jason 'Jay' Barnes (admitted *pro hac vice*)
jaybarnes@simmonsfirm.com
Eric Johnson (admitted *pro hac vice*)
ejohnson@simmonsfirm.com
An Truong (admitted *pro hac vice*)
atruong@simmonsfirm.com
112 Madison Avenue, 7th Floor
New York, NY 10016
Tel.: 212-784-6400
Fax: 212-213-5949

Dated: September 17, 2024

LOWEY DANNENBERG, P.C.

/s/ Christian Levis
Christian Levis

Christian Levis (admitted *pro hac vice*)
clevis@lowey.com
Amanda Fiorilla (admitted *pro hac vice*)
afiorilla@lowey.com
44 South Broadway, Suite 1100
White Plains, NY 10601
Tel: (914) 997-0500
Fax: (914) 997-0035

KIESEL LAW LLP

Jeffrey A. Koncius, State Bar No. 189803
koncius@kiesel.law
Nicole Ramirez, State Bar No. 279017
ramirez@kiesel.law
Kaitlyn Fry, State Bar No. 350768
fry@kiesel.law
8648 Wilshire Boulevard
Beverly Hills, CA 90211-2910
Tel: 310-854-4444
Fax: 310-854-0812

LIEFF CABRASER HEIMANN & BERNSTEIN, LLP

Michael W. Sobol (State Bar No. 194857)
msobol@lchb.com
Melissa Gardner (State Bar No. 289096)
mgardner@lchb.com
Jallé H. Dafa (State Bar No. 290637)
jdafa@lchb.com
275 Battery Street, 29th Floor
San Francisco, CA 94111-3339
Tel: 415 956-1000
Fax: 415-956-1008

Douglas Cuthbertson (admitted *pro hac vice*)
dcuthbertson@lchb.com
250 Hudson Street, 8th Floor
New York, NY 10013
Tel: 212 355-9500
Fax: 212-355-9592

SCOTT+SCOTT ATTORNEYS AT LAW LLP

Hal D. Cunningham (Bar No. 243048)
hcunningham@scott-scott.com
Sean Russell (Bar No. 308962)
srussell@scott-scott.com
600 W. Broadway, Suite 3300
San Diego, CA 92101
Tel: (619) 233-4565
Fax: (619) 233-0508

Joseph P. Guglielmo (admitted *pro hac vice*)
jguglielmo@scott-scott.com
Ethan Binder (admitted *pro hac vice*)

ebinder@scott-scott.com
230 Park Ave., 17th Floor
New York, NY 10169
Telephone: (212) 223-6444
Facsimile: (212) 223-6334

Attorneys for Plaintiffs and the Proposed Class

ATTESTATION

Pursuant to Civil Local Rule 5-1(h)(3), I hereby attest that all signatories listed, and on whose behalf the filing is submitted, concur in the filing's content and have authorized the filing.

Dated: September 17, 2024

/s/Jeffrey A. Koncius
Jeffrey A. Koncius